REMARKS/ARGUMENTS

The present amendment is submitted in accordance with the Revised Amendment Format.

The Examiner has rejected claims 1-6, 9-13, 18-19, 21-23, 25-27, 31, 35, 36, and 38-42 of this Application under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,657,538 to Ritter.

The Examiner has rejected claims 7, 8, 14-17, 24, and 32-34 of this Application under 35 U.S.C. § 103(a) as being unpatentable over Ritter in view of U.S. Patent No. 6,691,089 to Su et al. (herein, "Su").

The Examiner has rejected claims 20 and 37 of this Application under 35 U.S.C. § 103(a) as being unpatentable over Ritter in view of U.S. Patent No. 6,049,785 to Gifford.

The Examiner has rejected claims 28-30 of this Application under 35 U.S.C. § 103(a) as being unpatentable over Ritter in view of Su and further in view of U.S. Patent No. 6,700,953 to Maurer et al. (herein, "Maurer").

Independent claims 1 has been amended to more clearly define what Applicant regards as one embodiment of the invention.

Independent claims 31 has been amended to correct a typographical error.

All amendments are fully supported by the specification and no new matter has been added.

Interview Summary

On May 26, 2005, Applicant's Attorney conducted an interview with the Examiner. Applicants thank the Examiner for the interview. During the interview, the allowability of the claims was discussed. As set forth below, Applicants pointed out to the Examiner that Ritter does not disclose the invention as described by the claims (amended or unamended). The central issue discussed was whether or not (a) Ritter's disclosure of a biometric server including tables of biometric keys and (b) Ritter's disclosure of confirmation of biometric keys anticipates Applicant's independent claims (e.g., claim 1). In particular, Applicant's contended that Ritter does not disclose "security authorization" on *both* the client

and server that uses biometric data. Rather, as discussed in more detail below, Ritter only discloses use of biometric data for authorization on the client. In Ritter, the authorization on the server is a confirmation of the keys used to perform the client authorization, which is substantially different from what is claimed. Examiner and Applicant's Attorney reached an impasse on the issue.

Rejection under 35 U.S.C. § 102(b) based on Ritter

The issue in this case is whether or not Ritter anticipates the pending independent claims under Section 102.

A. Applicable Law:

"A claim is anticipated under 35 U.S.C. § 102 only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. V. Union Oil Co. of* California, 814 F.2d 628, 631 (Fed. Cir. 1987), MPEP 2131.01. The Federal Circuit has repeatedly emphasized that anticipation is established only if (1) all the elements of an invention, as stated in the patent claim, (2) are identically set forth, (3) in a single prior art reference. *In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997) ("To anticipate a claim, a prior art reference must disclose every limitation of the claimed invention, either expressly or inherently."); *In re Paulsen*, 30 F.3d 1475,1478-79 (Fed. Cir. 1994) ("A rejection for anticipation under section 102 requires that each and every limitation of the claimed invention be disclosed in a single prior art reference."); *Gechter v. Davidson*, 116 F.3d 1454, 1457 (Fed. Cir. 1997) ("Under 35 U.S.C. 102(b), every limitation of a claim must identically appear in a single prior art reference for it to anticipate the claim").

Importantly, the presence of each claim limitation in the disclosure of a reference must be clear. For example, as stated in *Datascope Corp. v. SMEC, Inc.*, "Anticipation cannot be predicated on teachings in a reference that are vague or based on conjecture." *Datascope Corp. v. SMEC, Inc.*, 776 F.2d 320 (Fed. Cir. 1985). This concept has been reiterated by the Board of Patent Appeals. For example, in *Ex parte Standish*, the Board stated, "anticipation of a

claimed product cannot be predicated on mere conjecture as to the characteristics of a prior art product." *Ex parte Standish*, 10 USPQ2d 1454, 1457 (Bd. Pat. App. & Int'f 1989).

B. Application of the Law and Reference to the Claims At-Issue:

The Examiner's rejection of independent claims 1, 9, and 31 of this Application under 35 U.S.C. § 102(e) as being anticipated by Ritter are not supported by the Ritter's disclosure. Applicants have amended claim 1 to more clearly distinguish the biometric data used for security authorization. Claims 1, 9, and 31 are allowable because Ritter does not clearly disclose each and every element recited in these claims either expressly or inherently.

1. Review of Ritter

Ritter discloses a system for securely obtaining, storing, and using "biometric keys" for authorization purposes. "The first recording of biometric keys is executed in a point of presence (POP)." Ritter, Col. 2, Lines 7-8. "From there, they are transmitted in a secure manner ... to a biometric server where they are stored in tables." Ritter, Col. 2, Lines 9-11. "The recorded and derived biometric keys of a client can be stored in a corresponding user profile." Ritter, Col. 3, Lines 11-12. Ritter goes on to reiterate that these biometric keys are sent to a server after initial creation at the point of presence. Ritter states as follows:

> "For completing the recording of the biometric keys, the user profiles or user group profiles with the biometric keys and the security information are transmitted by the program of the computer in a secured manner via a communication network 5 to a server for maintaining the biometric keys, in the following paragraphs referred to as biometric server 10, where they are stored for the respective user or user group in tables 11, connected 19 to the biometric server 10."

(Ritter, Col. 3, Lines 40-45).

Importantly, Ritter subsequently states that the biometric keys in the server and on the client are "*the same*."

> "The same information is likewise stored on the personal SIM card 3 of the user."

(Ritter, Col. 3, Lines 57-58).

It is in the context of this architecture that Ritter must be read. Ritter discloses authorization in column 4 in the context of a mobile phone with a SIM card having biometric keys stored thereon. Ritter states that:

> "The user can insert his personal SIM-card 3 in a communication terminal device 1 and turn on the device. In this example, the communication terminal device 1 is a mobile radio telephone, which is equipped with a video sensor 2 for recording body features."

(Ritter, Col. 4, Lines 26-30).

Ritter then discloses *one and only one set of biometric data received by the client*, which is used to generate "current biometric keys" on the client. The "current biometric keys" are then "compared to the stored biometric keys" to authorize the user on the client. Ritter additionally discloses that the "stored biometric keys" on the client can be "confirmed" on the server. The relevant portion of Ritter is as follows:

> "The data recorded by means of the video sensor 2 and, if applicable, by means of the microphone (not illustrated) of the mobile radio telephone 1, is temporarily stored by the authentication program. From this data, current biometric keys are derived which are temporarily stored and compared to the stored biometric keys 4. In addition to this direct comparison, the authenticity and the integrity of the stored biometric keys 4 can be confirmed by means of TTP services by the biometric server 10, for example. If the comparison of the current biometric key to the biometric key 4 stored in the SIM-card 3 turns out to be positive and if the stored biometric keys 4 are authenticated positively by the biometric server 10, further usage of the mobile radio telephone 1 may be permitted, for example. Otherwise, further usage of the mobile radio telephone 1 by this user may be prevented and the mobile radio telephone 1 may be turned off, for example."

(Ritter, Col. 4, Lines 32-48).

Thus, Ritter discloses storing the same biometric keys on the client and server, and obtaining one and only one set of biometric data to perform the authorization. In Ritter, the

only biometric data received from a user is used only once to generated "current biometric keys," which are compared to the stored biometric keys. This process is on the client only. Thus, biometric data is not used on the server. Rather, the stored biometric keys on the client (not the biometric data received from the user) are then checked to make sure they are still valid by "confirming" that they match the ones on the server. Applicants submit that this is substantially different from the embodiments of claims 1, 9, and 31.

2. Ritter does not anticipate amended claim 1

Amended claim 1 recites:

> "a client system receiving first and second biometric data from a user, the client system having a first level security authorization procedure, wherein the first level security authorization denies access to the client system if the first biometric data does not correspond to an authorized user; and
>
> a server system receiving the second biometric data from the client and having a second level security authorization procedure;
>
> wherein the first level security authorization procedure and the second level security authorization procedure comprise distinct biometric algorithms."

(Amended Claim 1)(Emphasis Added).

The first issue is whether or not Ritter discloses "a client receiving first and second biometric data from a user." Applicants contend that Ritter does not. Ritter discloses receiving one set of biometric data from the user to perform a security authorization – i.e., "current biometric data." Ritter's biometric keys are not received from the user, but rather, are stored in the SIM card and compared to the biometric keys derived from the "current biometric data." No other biometric data is received from the user for authorization. Thus, Ritter does not disclose "a client receiving first and second biometric data from a user" as required by claim 1. Because Ritter does not disclose a claim limitation of claim 1, Ritter does not anticipate claim 1 under Section 102.

The second issue is whether or not Ritter discloses "a server system receiving the second biometric data from the client." Applicants again contend that Ritter does not. Ritter

discloses that the stored biometric keys on the client are checked for "authenticity" and "integrity." However, the stored biometric keys on the client are not "second biometric data from a user." As mentioned in the previous Office Action Response, the specification discloses many embodiments of the first and second biometric data, including different types of biometric data, such as speech and fingerprints, or different portions of biometric data, such as a first and second portion of a single speech pattern. However, the specification does not disclose anything to suggest that the second biometric data the same biometric data (i.e., a biometric key) used to verify the first biometric data. Thus, Ritter does not disclose a server system receiving the second biometric data from the client" as required by claim 1. Because Ritter also does not disclose this claim limitation of claim 1, Ritter does not anticipate claim 1 under Section 102.

Claims 2-8 are dependent claims that include all the limitations of claim 1 and include additional limitations. Therefore, these claims are allowable for at least the same or similar reasons.

Claim 9 is allowable for similar reasons. For example, claim 9 recites:

> receiving a first level security authorization signal on the server system from a client system, wherein the first level security authorization signal indicates that the client system has authorized a user of the client;
>
> receiving biometric data on the server system from the client system;
>
> executing a second level security authorization, the second level security authorization including analyzing the biometric data using a first biometric algorithm on the server system; and
>
> generating a second level security authorization signal on the server system when the first biometric algorithm indicates that the biometric data corresponds to one of a plurality of users authorized to access the server system.

From the above discussion it should be clear that Ritter does not disclose "receiving a first level security authorization signal from a client" and "biometric data" and "executing a second level security authorization" on a server. As mentioned above, Ritter sends a "stored biometric key" used to authorize the client to the server to check for "authenticity" and "integrity" (i.e., to make sure the biometric key on the client is the same as the one on the server,

ostensibly to ensure that it has not been tampered with or changed). Moreover, authorization in Ritter cannot occur until the biometric keys stored on the client have been checked for "authenticity" and "integrity." Because Ritter does not include all the elements of claim 9, Ritter cannot anticipate claim 9 under 35 U.S.C. § 102(e).

Claims 10-30 are dependent claims that include all the limitations of claim 9 and include additional limitations. Therefore, these claims are allowable for at least the same or similar reasons.

Claim 31 is allowable for similar reasons. For example, claim 31 recites:

> receiving biometric data in the client system;
> analyzing a first portion of the biometric data using a first biometric algorithm on the client system, wherein the first biometric algorithm denies access to the client system if the first portion of biometric data does not correspond to an authorized user;
> generating a first level security authorization signal on the client system when the first biometric algorithm indicates that the first portion of the biometric data corresponds to an authorized user;
> transmitting the first level security authorization signal and a second portion of the biometric data to a server system, the second portion of biometric data being analyzed by a second biometric algorithm on the server; and
> accessing resources on the server system through the client system when the second biometric algorithm provides a second level security authorization.

As mentioned above, Ritter does not disclose a biometric algorithm that denies access to the client system if the first portion of biometric data does not correspond to an authorized user. Furthermore, Ritter does not disclose generating a "security authorization signal" on a client "when the first biometric algorithm indicates that the first portion of the biometric data corresponds to an authorized user." Moreover, Ritter does not disclose analyzing a first portion of biometric data on a client using a first biometric algorithm and transmitting a second portion of biometric data and a security authorization signal to the server. Thus, Ritter

does not include all the elements of claim 31, and cannot anticipate claim 31 under 35 U.S.C. § 102(e).

Claims 32-42 are dependent claims that include all the limitations of claim 31 and include additional limitations. Therefore, these claims are allowable for at least the same or similar reasons.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 408-244-6319.

Respectfully submitted,

Chad R. Walsh
Reg. No. 43,235

FOUNTAINHEAD LAW GROUP
900 Lafayette Street, Suite 509
Santa Clara, CA 95050
Tel: 408-244-6319
CRW